UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 16310 MARVENE DRIVE, HACIENDA HEIGHTS, CALIFORNIA	)	Case No. 2:18-MJ-03083

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 371, 1001, 1349, 1341, 1956, and 31 U.S.C. § 5324	See attached Affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

Postal Inspector Kelly Shen
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

_____
Judge's signature

City and state: Los Angeles, California

The Honorable John E. McDermott, U.S. Magistrate Judge
Printed name and title

AUSA Andrew Brown, x0102, 11th Floor

ATTACHMENT A – ARRIBENO RESIDENCE

The premises to be searched is:

16310 MARVENE DRIVE, HACIENDA HEIGHTS, CALIFORNIA, 91745 ("ARRIBENO RESIDENCE"). The ARRIBENO RESIDENCE is a two-story, single-family home. The ARRIBENO RESIDENCE is located on the south side of MARVENE DRIVE, and is east of Country Canyon Road. The ARRIBENO RESIDENCE is tan in color with light green trim. There is an attached two-car garage with a light green garage door that faces north. A concrete driveway wide enough for two cars leads directly to the attached garage. The front door faces north. There are black numbers "16310" to the right of the entryway, as well as on the curb in front of the house. The premises to be searched includes vehicles parked in the driveway and garage. The ARRIBENO RESIDENCE is further described by the attached photograph.

ARRIBENO RESIDENCE

ATTACHMENT B

I. ITEMS TO BE SEIZED FROM THE RESIDENCES AND SAFETY DEPOSIT BOX

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S. Code §§ 371, 1001, 1349, 1341, 1956, and 31 U.S. Code § 5324 (Conspiracy to Defraud the United States Government, False Statements, Conspiracy to Commit Mail Fraud, Money Laundering, and Structuring), namely:

a. Records referring or relating to the submission of mail by "PREMIER MAILING, INC.", also known as ("aka") "PREMIER MAILING SERVICES", aka "PREMIER PRINTING AND MAILING", aka "PREMIER" (referred to hereafter as "PREMIER"), to the USPS or the postage payment method from January 1, 2014, onward;

b. Records relating to the ownership structure of PREMIER, its owners and/or shareholders, and employees;

c. Records relating to revenue and income received by PREMIER including ledger, cashbooks, bank statements, financial records, and computerized account records from January 1, 2014, onward;

d. Documents and records referring or relating to financial transactions between at least two of PREMIER, RAMON ARRIBENO ("ARRIBENO"), ARMANDO LOPEZ ("LOPEZ"), Wanda Weaver, and JUAN CAUDILLO ("CAUDILLO"), from January 1, 2014, onward;

e. Communications between PREMIER or its employees, owners and representatives on the one hand, and CAUDILLO on the other hand;

f. Communications between at least two of PREMIER, ARRIBENO, LOPEZ, Wanda Weaver, and CAUDILLO referring or relating to: sharing or splitting sums of money; or opaque or coded messages, such as those omitting units (e.g., "I gave it to him," or "you owe me 4");

g. Records referring or relating to: postal audits or bank or other investigations; banks or other financial institutions terminating accounts; routing payments through third parties or businesses, or otherwise disguising payments or the source of funds; changing or incorrect mailing or other records; CAUDILLO's work schedule and timing mailings to coincide with it; payments and gifts, or amounts owed, to CAUDILLO; Logan Advertising or J.C. Greenhouse; payments, including in-kind payments such as the free or below-market use of a house, to or from LOPEZ, other than his paycheck; structuring cash transactions to keep them below $10,000; ways of cheating the post office out of revenue and hiding that fraud;

h. Records relating to wealth and the movement of wealth since January 2014, such as brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashier's checks, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and

investments, or showing or referring to purchases or transactions for more than $10,000;

i. Documents and keys relating to safety deposit boxes and public storage units;

j. Currency if it exceeds $1,000, and records referring or relating to currency transactions over $1,000;

k. Documents and records showing email and telephone contacts and numbers called, such as SIM cards, address books, call histories, and telephone bills;

l. Records or items containing indicia of occupancy, residency, control or ownership of any location or vehicle being searched, such as leases, utility bills, identity documents, and cancelled mail;

m. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

n. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mails, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. Evidence of the presence or absence of

software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified,

or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras, gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search tem shall complete the search as soon as is practicable but

not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 120-day period without first obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine where the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

d. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

e. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access data falling outside the scope of the items to be seized (after the time for searching the device has expired) absent further court order.

f. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

g. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. If ARRIBENO, LOPEZ, or CAUDILLO is located at the premises being searched and is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device found there that falls within the scope of the warrant, then law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of that person onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front

of the face of the person with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any other search of the digital devices.

A F F I D A V I T

I, Kelly Shen, being duly sworn and under oath, hereby depose and say as follows:

INTRODUCTION

1. I am a Postal Inspector with the United States Postal Inspection Service, Los Angeles Division, Los Angeles, California. I became a Postal Inspector in 2005. For approximately one year from 2006-2007, I worked as a Special Agent with the United States Postal Service Office of Inspector General. In 2007, I returned to work as a United States Postal Inspector. I completed a twelve-week basic training course in Potomac, Maryland. Since 2007, I have been assigned to the Revenue Investigations Team, which is responsible for investigating fraud against the United States Postal Service ("USPS" or "Postal Service"). Based on my training, experience, and discussions with other Postal Inspectors, I am familiar with the rules and regulations governing the USPS, including those pertaining to the acceptance, classification, sorting and delivery of mail; the methods used to commit fraud against the USPS; and the documents and other records that frequently evidence such fraud. I have participated in or conducted recent criminal investigations concerning mail acceptance procedures, scheme that defraud the USPS of the lawful payment of postage.

PURPOSE OF AFFIDAVIT: SEARCH WARRANTS

2. This affidavit is made in support of search warrants of the business site of PREMIER MAILING INC. ("PREMIER"), the residence and safety deposit box of RAMON ARRIBENO ("ARRIBENO"), the owner of

PREMIER, the residence of ARMANDO LOPEZ ("LOPEZ"), a manager at PREMIER, and the residence of JUAN CAUDILLO ("CAUDILLO"), a USPS employee for evidence of violations of Title 18, United States Code, Sections 371, 1001, 1349, 1341, 1956 (Conspiracy to Defraud the United States Government, False Statements, Conspiracy to Commit Mail Fraud and Money Laundering), namely, a scheme in which PREMIER, through ARRIBENO and LOPEZ, appears to bribe the postal employee responsible for vetting their bulk mailings, CAUDILLO, to falsely log those mailings as prepaid when in fact they were not, resulting in millions of dollars in lost revenue to the Post Office:

a. 14522, 14524 AND 14526 GARFIELD AVENUE, PARAMOUNT, CALIFORNIA ("PREMIER");

b. 16310 MARVENE DRIVE, HACIENDA HEIGHTS, CALIFORNIA ("ARRIBENO RESIDENCE");

c. 4445 JASPER STREET, LOS ANGELES, CALIFORNIA ("LOPEZ RESIDENCE");

d. 6223 TANGLEWOOD STREET, LAKEWOOD, CALIFORNIA ("CAUDILLO RESIDENCE");

e. SAFETY DEPOSIT BOX NUMBER 0010412-5, U.S. BANK, 15943 PARAMOUNT BOULEVARD, PARAMOUNT, CALIFORNIA ("SAFETY DEPOSIT BOX");

3. Collectively, the premises to be searched are referred to as the SUBJECT PREMISES, and are described in more detail in the Attachments A, which are incorporated.

PURPOSE OF AFFIDAVIT: ASSET SEIZURE WARRANTS

4. This affidavit is also made in support of an application for a seizure warrant for the balance of the following U.S. Bank Account numbers associated with PREMIER and its owner ARRIBENO:

a. 1-534-5867-2505, in the name of Premier Mailing Inc.(“**U.S. Bank Account 2505**”);

b. 1-575-1597-2683, in the name of Premier Printing & Mailing Inc. (“**U.S. Bank Account 2683**”);

c. 1-575-1597-2709, in the name of Premier Printing & Mailing Inc. (“**U.S. Bank Account 2709**”);

d. 1-575-1597-2717, in the name of Premier Printing & Mailing Inc. (“**U.S. Bank Account 2717**”);

e. 1-575-1762-6311, in the name of Ramon Arribeno (“**U.S. Bank Account 6311**”).

5. This affidavit is also made in support of an application for a seizure warrant for the balance of the following Wells Fargo Bank Account numbers associated with CAUDILLO (which do not include the account into which his postal pay is deposited):

a. 6300211890, in the name of Juan E. Caudillo DBA J.C. Trucking (“**Wells Fargo Account 1890**”);

b. 6351146631, in the name of Juan E. Caudillo (“**Wells Fargo Account 6631**”);

c. 9218515014, in the name of Juan E. Caudillo DBA J.C. Greenhouse (“**Wells Fargo Account 5014**”);

d. 6885605284, in the name of Juan E. Caudillo DBA J.C. Greenhouse (“**Wells Fargo Account 5284**”).

6. The above listed accounts, collectively referred to as the SEIZEABLE ACCOUNTS, are subject to seizure and forfeiture to the United States because there is probable cause to believe that they constitute and are derived from proceeds traceable to the fraud and money laundering schemes, and are therefore subject to seizure pursuant to 21 U.S.C. § 853(f), 18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), 21 U.S.C. § 853, and 18 U.S.C. § 984.

7. The information set forth in this affidavit is based upon my participation in the investigation, encompassing my personal knowledge, observations and experience, as well as information obtained through my review of evidence, investigative reports, interviews, and information provided by other participating law enforcement agents. As this affidavit is being submitted for the limited purpose of securing the requested warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrant.

INVESTIGATION BACKGROUND

8. The investigation revealed a scheme where PREMIER used false statements to defraud the USPS of proper postage payment. As described below, my investigation demonstrated PREMIER claimed to submit mailings to the USPS which had postage affixed to the mail. However, PREMIER did not affix postage to the mailings causing a documented loss to the USPS of approximately $3,000,000 (the actual loss is probably much higher but I cannot calculate it without the records I hope to get with the search warrants this affidavit

seeks). It appears there is collusion between ARRIBENO and LOPEZ as the owners / operators of PREMIER and CAUDILLO, the USPS employee assigned to review PREMIER's mail, to falsely certify the mail has been affixed with prepaid metered postage.

Premier Background

9. Based on my investigation I know PREMIER is a third-party mailing company. I reviewed the website for PREMIER and learned PREMIER offers services to their customers including: mail piece design, printing, addressing, postage application, mail sorting and transportation. Some of Premier's clients include marketing companies, real estate companies, and political mailers who use PREMIER to print and mail advertisements on their behalf.

10. Based on my training and experience, I know that third-party mailers such as PREMIER typically maintain business records pertaining to mailings at their place of business. These records usually include postage statements and any supporting documentation, invoices showing amounts they charged their customers for services and postage, copies of mail pieces and correspondence with customers and the post office.

11. Based on my training and experience, I know businesses such as PREMIER typically do not operate in cash. Most third-party mailers receive payments from their customers in the form of check or credit payment. I reviewed documents from Banc of California for account numbers ending in 5237, 9425 and 3117 held by PREMIER. I observed checks deposited into these accounts from customers of PREMIER ranging in amounts from approximately $100 to $100,000.

ARRIBENO Owns PREMIER

12. I queried State of California Business records and learned PREMIER became incorporated in California in 2001, under entity number C23525355. ARRIBENO is listed as the agent for processing and the Chief Executive Officer for PREMIER. I queried law enforcement databases which named ARRIBENO as the owner of PREMIER. Public records and law enforcement databases show the address for PREMIER as 14522 Garfield Avenue, Paramount, California. On or around November 19, 2018, I spoke with a representative of the property manager for the premises occupied by PREMIER and learned PREMIER occupies 14522, 14524 and 14526 GARFIELD AVENUE, PARAMOUNT, CALIFORNIA.

13. On several occasions including April 10, 2017, May 1, 2017, and July 2, 2018, USPS Office of Inspector General ("USPS OIG") Special Agent Brian Rudolph ("SA Rudolph") or I observed vehicles registered to ARRIBENO parked in front of PREMIER in a parking space marked for ARRIBENO. In my training and experience, this is indicative that ARRIBENO is an active participant in the day to day business activities of PREMIER.

14. I learned through a review of USPS records that PREMIER has done business with the USPS since approximately 1999. I also learned PREMIER holds a permit to process bulk mail at the Paramount, California Post Office, located approximately half a mile from the PREMIER PREMISES. ARRIBENO is listed as a contact for the USPS account. "Bulk mail" is a USPS term used to describe mailings

submitted in large quantities, usually by third-party mailers (such as PREMIER) on behalf of their customers.

Paramount Post Office

15. CAUDILLO is the primary USPS employee who works at the Paramount bulk mail unit--where mail from PREMIER is verified. According to USPS records, CAUDILLO became a "Bulk Mail Technician" in 1991 and has remained in that position throughout his employment with the USPS. There is a "back-up" clerk at the Paramount Post Office who will verify the mail if CAUDILLO is out of the office or can assist CAUDILLO if there is a high volume of mail on a particular day. SA Rudolph advised me he reviewed USPS records and CAUDILLO's records with the Department of Motor Vehicles and confirmed CAUDILLO's address is the CAUDILLO RESIDENCE. SA Rudolph advised me he did surveillance at the CAUDILLO RESIDENCE on October 15, 2018, and observed CAUDILLO at the CAUDILLO RESIDENCE.

PROBABLE CAUSE

Case Initiation

16. On or around June 6, 2016, USPS OIG Special Agent Jill Brock ("SA Brock") and I met with a cooperating witness ("CW"). The CW wanted to meet with USPS investigators because the CW believed PREMIER is defrauding the postal service of proper postage payment.

17. On or around July 27, 2016, SA Rudolph and I met with the CW. The CW advised that he/she believes an employee of PREMIER, LOPEZ, is defrauding the USPS by altering postage statements. The CW believed that CAUDILLO was helping PREMIER defraud the USPS in the processing of mailings.

Comparison Of Mailing Records Shows Fraudulent Activity

18. Starting around July 2016, I began to review entry forms submitted by PREMIER at destination USPS facilities in Southern California. (The USPS gives mailers like PREMIER a discount on postage if they deposit their mail at a USPS facility close to its final destination. Mailers must submit an entry form with the mail to document the verification and payment of postage at the origin post office, Paramount Post Office in this case.)

19. I compared the destination forms to the originating paperwork which SA Rudolph and/or I obtained from the Paramount Post Office. I found there were discrepancies with the postage payment method. The originating forms we obtained at the Paramount Post Office listed the payment method as metered postage, while the destination forms listed the postage payment method as permit imprint. This is important because metered postage is prepaid. Permit imprint postage is not prepaid and must be paid at the time of mailing.

20. From my training and experience, I know that a common way third-party mailers such as PREMIER could defraud the USPS is by claiming their postage was pre-paid with metered postage, when in fact there was no metered postage affixed to the mail pieces, having the effect of mailing the items without any payment to the USPS. I also know that the postage payment section of the form is supposed to be completed by the USPS employee verifying the mailing. As the payment method is completed by the USPS employee, inconsistent

completion of the form is indicative of USPS employee involvement resulting in the mailer not submitting proper postage payment.

21. In October 2016, I requested to have Inspectors throughout the country search for destination forms for PREMIER at their respective destination USPS facilities. Once I obtained the forms from the other locations, I compared them to the originating PS Forms 8125 and postage statements from the Paramount Post Office. From approximately December 2015, through July 2016, I found over 200 forms that had postage payment method discrepancies. The postage payment method listed metered postage on the originating form and permit imprint on the destination form. The estimated loss associated to these mailings was approximately $869,842.

22. From approximately September 2016 through the present, SA Rudolph and I continued to collect copies of originating postal forms from the Paramount Post Office files and destination postal forms from Southern California USPS facilities. During that time frame, we found approximately 191 additional destination PS Forms 8125 that had the same postage payment discrepancy as the earlier forms. The loss attributed to these additional discrepancies is approximately $948,279. Based on my training and experience, I believe there are more instances of fraudulent mailings done by PREMIER, but I do not have the records to conduct a complete analysis. I also know business such as PREMIER maintain records that could be used to complete the analysis necessary to determine the breadth of the fraud. Based on my review of the current documentation, I learned the following:

a. There were consistent fraudulent mailings submitted by PREMIER. Listed below is a sample of dates of fraudulent mailings submitted by PREMIER during the most recent five months for which I have the best records:

i. March 2nd, March 9th, March 12th, March 15th and March 16th, 2018.

ii. April 6th, April 9th, April 11th, April 12th, April 13th, April 24th April 26th and April 30th, 2018.

iii. May 2nd, May 4th, May 8th, May 9th, May 10th, May 11th, May 14th, May 15th, May 16th, May 18th, May 22nd, and May 30th, 2018.

iv. June 5th, June 12th, and June 19th, 2018.

v. July 3rd, July 17th, July 23rd and July 31st, 2018.

b. Logan Advertising is a customer of PREMIER. A large portion of the fraudulent mailings submitted by PREMIER were mailings submitted on behalf of Logan Advertising. Based on my training and experience, I know that some advertising and marketing companies do not request or thoroughly review paperwork from the third-party mailers they use to mail on their behalf. It is easier for third-party mailers to conduct the fraud scheme when they know their customers are not scrutinizing the USPS documentation. Some third-party mailers will “test the waters” with their customers to determine which customers review paperwork and which customers do not request USPS documentation. PREMIER’s fraud was not just limited to Logan, I also observed fraudulent mailings done by

PREMIER on behalf of additional customers such as real estate agents, and political mail.

Comparison of Records to Determine Start of Scheme

23. I initially identified the fraudulent mailings by comparing the origin and destination postal forms. The USPS has a limited retention policy for these forms. I also reviewed records provided by Hasler / Neopost, an approved USPS meter provider. I compared meter usage records provided by Hasler / Neopost versus the USPS records of reported metered mailings done by PREMIER. I was able to review records as far back as 2014, and observed an approximate $1.1 million discrepancy in 2014. Since the discrepancies occurred in the earliest records I was able to review, it is likely the fraud began prior to 2014. I anticipate losses exceeding my current $3 million estimation as I am limited to a review of records that I have in my possession. Based on my training and experience, I know mailers such as PREMIER maintain documents and records at their place of business that can facilitate a more comprehensive loss calculation. I also know that participants in a scheme to defraud may keep records of the fraud at their residence where it is not easily discoverable by associates not participating in the fraud.

Spot Checks of PREMIER'S Mailings Show PREMIER Falsely Claimed Metered Postage

24. On or around the following dates, a USPIS contractor and/or I located PREMIER'S mailings at destination USPS facilities. We reviewed the physical mail and compared it to the record of the

mailing in the USPS computerized tracking system. The postage statement and origin postal forms stated postage was paid via prepaid metered postage. The destination entry forms which accompanies the mail to its final destination claimed the postage was paid via permit imprint. In each observation, I did not observe any metered postage affixed to the mail; rather, the mail bore a permit imprint indicia. This is important because permit imprint is not prepaid and must be paid at the time of mailing. As a result of these false claims, the USPS was not paid properly for these mailings. Listed below are the dates of the mailings and the approximate loss amounts:

a. January 18, 2017 - $1,100.

b. March 16, 2017 - $2,349.15.

c. May 12, 2017 - $7,000.

d. July 6, 2017 - $24,494.61.

e. November 28, 2017 - $27,148.50.

f. May 8, 2018 - $9,492.69.

g. May 14, 2018 - $3,405.91.

h. June 5, 2018 - $19,035.09.

i. June 19, 2018 - $31,228.62.

j. August 14, 2018 - $17,311.70.

k. August 21, 2018 - $17,511.46.

l. August 28, 2018 - $22,406.26.

m. September 4, 2018 - $21,544.57.

n. September 18, 2018 - $25,267.60.

25. On our around the dates of each mailing, I reviewed USPS databases and determined each of the mailings were processed at the Paramount Post Office by CAUDILLO. The USPS databases also listed the payment method for each of the mailings as metered postage.

San Francisco Mail Review Shows Additional Fraud

26. On April 12, 2018, I reviewed USPS databases and saw PREMIER submitted a metered mailing that was destined for a San Francisco, CA USPS facility. I contacted Postal Inspector Alex Hill from the San Francisco Division of the Postal Inspection Service and requested he review the mail from PREMIER upon its arrival. On April 13, 2018, Inspector Hill located the mail from PREMIER. Inspector Hill told me the mail bore a permit imprint and he did not observe any metered postage affixed to the mail. Inspector Hill took pictures of the mail and sent them to me.

CAUDILLO SHOULD HAVE SEEN THE POSTAGE TYPE WAS PERMIT

27. I reviewed the photographs sent to me from Inspector Hill and observed that one of the mail pieces had a stamp on the envelope which read, “Opened for Inspection by the USPS”. The stamp was just below where the permit imprint marking is located on the mailing. From my training and experience, I know that during the mail acceptance procedure, USPS policy requires the clerk, when prompted, to open at least one piece of mail for inspection. I reviewed USPS documentation which showed CAUDILLO was the USPS clerk who performed the verification for this mailing. I reviewed USPS databases which also showed CAUDILLO was the USPS clerk who verified in the USPS computerized tracking system that the mailing was paid via metered

postage, when in fact the mailing bore indicia for a permit mailing. As the stamp was placed just below the permit imprint marking, I believe CAUDILLO would have seen the mail was not affixed with metered postage as PREMIER claimed. The loss to the USPS from this mailing was $4,086.68.

CAUDILLO is the USPS Clerk Who Verified Every Fraudulent Mailing

28. I reviewed USPS records submitted by PREMIER and observed that PREMIER has permit accounts at several post offices throughout Southern California. The only time I observed the fraudulent payment classification is when CAUDILLO verified the mail. I did not observe any fraud on mailings verified by the "back-up" clerk, or at other post offices. Based on my training and experience I know that third-party mailers attempting to defraud the USPS for the purpose of financial gain typically need the assistance from a USPS employee to execute the scheme.

CAUDILLO Cancelled a Permit Imprint Mailing and Re-entered it as Metered to Perpetuate the Fraud

29. On or around May 15, 2018, I reviewed USPS databases and saw PREMIER made a metered mailing of 15,004 pieces on May 14, 2018. A USPIS contractor reviewed the mailing at a USPS facility in Los Angeles, California and observed it was not affixed with metered postage. The mail bore a permit imprint. As stated above, this had the effect of not collecting payment for this mailing, causing a loss to the USPS of approximately $3,405.91.

30. During my review of USPS databases, I observed this mailing was initially entered as a permit imprint payment method.

However, the initial entry was cancelled by "JEC". An identical postage statement was entered into the USPS database, however, this postage payment method was metered postage. The re-entered postage statement was also verified by "JEC". I know from my discussion with USPS management that "JEC" is the username for CAUDILLO in the USPS database.

CAUDILLO Falsified USPS Documents to Maintain the Fraud

31. During my review of postal forms, I found a form with an error. The form was missing CAUDILLO's signature as the verifying USPS employee. The form was dated May 16, 2018, and the mail was destined for Los Angeles, California. The USPS clerk accepting the mail in Los Angeles observed the missing signature and notated on the form that they called the Paramount Post Office and spoke with CAUDILLO, who verified the payment and acceptance of the mail. The postage payment method on the destination form going to Los Angeles was checked as permit imprint. Attached to the destination entry form was a faxed copy of the originating form from the Paramount Post Office. The fax came from the Paramount Post Office on May 16, 2018, at 5:39 P.M. The faxed originating copy shows a checkmark next to permit imprint, and a lighter checkmark next to metered postage, suggesting that it was initially checked (falsely) as metered, but then erased and marked as permit imprint so that the honest postal employee receiving the fax would not detect the scheme.

32. I reviewed USPS databases and observed CAUDILLO accepted this mailing on May 16, 2018. The postage payment method was

metered postage. I also found a second postal entry form associated to this mailing going to City of Industry, California. The originating form indicated metered postage was paid. The destination entry form which accompanied the mail to City of Industry indicated permit imprint was the method of payment. The loss to the USPS from this mailing was approximately $5,341.43.

LOPEZ and CAUDILLO's Frequent Communication

33. SA Rudolph reviewed records for telephone number 562-547-1397, associated to CAUDILLO from the period of July 19, 2017, through July 3, 2018. SA Rudolph identified CAUDILLO's cellular telephone number through USPS employee records. SA Rudolph also identified 562-449-8931, a cellular telephone number associated to LOPEZ through law enforcement databases. SA Rudolph observed there were approximately 155 phone calls to or from phone number 562-449-8931 (the cellular telephone number associated to LOPEZ.) There were also approximately 119 text messages exchanged between the phone numbers associated to CAUDILLO and LOPEZ.

34. In the review of the records, SA Rudolph also observed the phone number associated to CAUDILLO called the phone number associated to LOPEZ on April 10, 2018, at approximately 2:11 p.m. This is significant because I learned from USPS management that on April 10, 2018, the USPS conducted an audit at the Paramount Post Office bulk mail unit where CAUDILLO works. (Post Offices are periodically audited by the USPS to ensure proper protocols are being followed). The Paramount bulk mail unit generally opens for business at 3:00 p.m.

35. SA Rudolph's review of CAUDILLO's cellular telephone records also identified telephone calls and or text message exchanges between CAUDILLO and telephone numbers identified through law enforcement databases as being affiliated with other mailers who utilize the Paramount Post Office's bulk mail unit, some of whom are suspected in other fraud schemes involving CAUDILLO.

Relationship between PREMIER and CAUDILLO

36. Throughout the course of the investigation, I spoke with several USPS employees regarding the Paramount Post Office. USPS employees advised me of the following information:

a. CAUDILLO would either call mailers on the day of the audit to warn them of the audit, or ask another employee to call the mailers on his behalf.

b. Other mailers in Paramount complained that CAUDILLO gave PREMIER preferential treatment.

LOPEZ'S Name is Associated to the Fraudulent Documents

37. During my review of postal forms, I observed that ARMANDO LOPEZ was listed as the mailer contact name on the USPS entry forms, including the fraudulent forms.

"ADL" [ARMANDO LOPEZ] Changed the Postage Payment Method

38. On or around November 29, 2017, I reviewed USPS databases for mailings done at Paramount on November 28, 2017. I observed PREMIER cancelled a permit imprint mailing they electronically submitted for 120,660 pieces. I reviewed the cancelled report and observed it stated it was cancelled by "ADL", which I believe are the initials for ARMANDO LOPEZ. A mailing with the same

characteristics to include number of pieces, piece weight, and client was re-entered as being paid with metered postage. As described above, we reviewed this mailing and did not observe any metered postage affixed to the mail pieces. The loss to the USPS was $27,148.50.

39. In our interview with the CW on July 27, 2016, the CW stated LOPEZ changed the postage statements.

40. On or around July 5, 2018, I conducted a phone call to LOPEZ at PREMIER. LOPEZ stated he is the plant manager at PREMIER. LOPEZ stated he prefers to use manual postage statements because sometimes clients change the number of pieces they wish to mail and then they have to cancel the electronic postage statement submission. LOPEZ stated it is easier for him to use manual postage statements. LOPEZ stated there is another employee who helps him with the electronic postage statements, but his primary job is to complete the manual postage statements.

a. The information is important because there were no changes made to the cancelled postage statement other than the postage payment method. Based on my training and experience, I know mailers do sometimes cancel a postage statement when they entered incorrect information. Usually, the erroneous information has been changed on the resubmission of the paperwork. In this instance, the only feature that changed was the postage payment method in an effort to further the fraud.

LOPEZ lives in a house owned by ARRIBENO

41. During my search of law enforcement databases, I found ARRIBENO owns the ARRIBENO RESIDENCE, which I believe is his primary residence based on my query of Department of Motor Vehicle ("DMV") records. I also conducted surveillance at the ARRIBENO RESIDENCE on October 6, 2018, and observed a Mercedes with California license plate 7KFK930, and a Porsche with California license plate 7W0S313 parked in the driveway of the ARRIBENO RESIDENCE. I obtained records from a law enforcement database which showed both vehicles are registered to ARRIBENO. Law enforcement databases also showed ARRIBENO as the owner of the LOPEZ RESIDENCE. DMV records show LOPEZ resides at 4445 Jasper Street, Los Angeles, California. I conducted surveillance on September 17, 2018, and September 18, 2018, at the LOPEZ RESIDENCE and observed a Honda sedan bearing California license plate 7MLW570 parked in the driveway of the LOPEZ RESIDENCE. On February 8, 2017, I learned from a query of law enforcement databases that a 2015 Honda with California license plate 7MLW570 is registered to LOPEZ at the LOPEZ RESIDENCE. On October 18, 2018, I conducted surveillance at the LOPEZ RESIDENCE and observed a Cadillac with California license plate 8GBA420 parked in the driveway. I learned from a query of law enforcement databases that this vehicle is registered to LOPEZ at the LOPEZ RESIDENCE.

ARRIBENO Makes Large Payments to LOPEZ

42. I reviewed documents for Banc of California business checking accounts ending in 5237, 9425 and 3117 held by PREMIER.

All three accounts listed ARRIBENO as the sole authorized signer. I learned account ending in 5237 was opened on or around July 14, 2009. Account ending in 9425 was opened on or around January 23, 2006. Account ending in 3117 was opened on or around May 7, 2012. I reviewed the documents and observed some expected business activity in these accounts, such as payments from clients of PREMIER, and payments from PREMIER to their vendors, including the USPS. From my review of the documents, I also observed that from November 2014 through March 2017, over $2 million in payments were made to LOPEZ in addition to his regular salary. I documented approximately 283 payments during that time frame. All of the payments were checks written for under $10,000. Most of these payments to LOPEZ were negotiated for cash.

43. I reviewed documents for Banc of California checking account number ending in 1126 for a personal account held by LOPEZ opened on or about March 2004. I learned the sole authorized signer on the account was listed as LOPEZ. I observed the account had very little activity. Some payroll checks from PREMIER were deposited into LOPEZ's account, however, LOPEZ typically immediately withdrew the majority of the payment for cash. The account maintained a low balance, usually under $1,000.

Suspicious Activity in ARRIBENO's Personal Bank Account

44. I reviewed documents for Banc of California checking account number ending in 9896 held by ARRIBENO. I learned this account was opened on or about November 15, 2005, and had ARRIBENO listed as the signatory. I found this account had substantially

more activity than LOPEZ's account. I learned there were frequent cash deposits in amounts under $10,000 into ARRIBENO's account. For example, I reviewed statements from January 2017 through October 2017 and found there were 22 cash deposits totaling approximately $164,000.

45. I also found there were numerous funds transfers between personal accounts held by ARRIBENO and business accounts held by PREMIER. For example, I reviewed documents from 2017 and observed there were five checks written from ARRIBENO's personal account ending in 9896 to business accounts for PREMIER totaling approximately $100,000.

46. Based on my training and experience, I know that people who are attempting to conceal fraudulently obtained income will attempt to keep cash transactions under $10,000 to avoid financial industry reporting requirements. Suspects involved in fraud often structure cash deposits and withdrawals to avoid mandatory financial institution generated reports that can later be reviewed by law enforcement personnel. I also know that people who generate large sums of money from their fraud often launder the proceeds of their fraud to make them appear legitimate or put them beyond the reach of law enforcement. Typically this is done by wiring or depositing cash into bank accounts or other investment vehicles such as brokerage accounts or real property.

47. Banc of California subsequently closed accounts belonging to PREMIER, ARRIBENO AND LOPEZ due to suspicious activity.

Identification of Current Bank Accounts

48. I reviewed USPS records and learned that PREMIER is currently using **U.S. Bank Account 2683** to pay for postage.

49. On or around November 6, 2018, I reviewed records from U.S. Bank and learned the following accounts are registered to PREMIER and/or ARRIBENO:

a. **U.S. Bank Account 2505** registered to PREMIER was opened on December 13, 2006. This account has a current balance of $197.03.

b. **U.S. Bank Account 2683** registered to PREMIER was opened on December 13, 2017. This account has a current balance of $68,150.53.

c. **U.S. Bank Account 2709** registered to PREMIER was opened on December 13, 2017. This account has a current balance of $87,033.06.

d. **U.S. Bank Account 2717** registered to PREMIER was opened on December 13, 2017. This account has a current balance of $907.72.

e. **U.S. Bank Account 6311** registered to ARRIBENO was opened on May 7, 2018. This account has a current balance of $35,010.18. I completed a brief review of this account and learned that from May through October of 2018, there were approximately 14 transfers from **U.S. Bank Account 2683** and **U.S. Bank Account 2709** into **U.S. Bank Account 6311**. These transfers totaled approximately $160,815.00. I also observed payroll checks from “ADP” that are marked for payroll. Therefore, it does not appear these fund

transfers are into ARRIBENO's purportedly personal account (**U.S. Bank Account 6311**) are his pay. I also observed six checks written from ARRIBENO on **U.S. Bank Account 6311** to Wanda Weaver from June through October 2018. These checks totaled approximately $25,822.74. This is significant because the CAUDILLO RESIDENCE is owned by Wanda Weaver. SA Rudolph advised me Wanda Weaver is listed as an emergency point of contact on CAUDILLO's USPS employee records. SA Rudolph also advised me he reviewed law enforcement records which show Wanda Weaver purchased the CAUDILLO RESIDENCE in 1999. On October 15, 2018, I conducted surveillance at the CAUDILLO RESIDENCE and observed a vehicle with California license plate B082N0 parked in the driveway. I reviewed a law enforcement report which shows this vehicle is registered to Wanda Weaver at the CAUDILLO RESIDENCE. I have not found any association between PREMIER and Wanda Weaver. Based on my training and experience, I know that it is common for illicit payments such as kickbacks or bribes to be made to someone associated with the person to whom the payment is intended, such as a spouse or family member, as a means of preventing the discovery of the bribes.

f. I also later learned from U.S. Bank records that SAFE DEPOSIT BOX NUMBER 0010412-5 was opened by RAMON ARRIBENO on May 8, 2018, and is located at U.S. BANK, PARAMOUNT BRANCH, 15943 PARAMOUNT BOULEVARD, PARAMOUNT, CALIFORNIA 90723 (the "SAFETY DEPOSIT BOX").

Suspicious Activity in CAUDILLO's Bank Accounts

50. SA Rudolph advised me he reviewed documents for Wells Fargo bank accounts ending in 1890, 5014, 5585, 8167, 0543, 4265,

5284, and 6631. SA Rudolph provided me with the following information based on his review of the above listed accounts:

a. The accounts included checking and savings accounts held personally by CAUDILLO, including jointly with his children, and held by entities listed as CAUDILLO "doing business as" various entities.

b. CAUDILLO's paycheck from the USPS is direct deposited into Wells Fargo Account 5585 and had a balance of $32,255.30 as of June 30, 2018. (This affidavit does not seek the seizure of this account).

c. **Wells Fargo account 1890** was initially opened on May 4, 2010, had a balance of $15,469.57 as of June 30, 2018.

d. **Wells Fargo account 6631** was initially opened on June 21, 2010, had a balance of $9,146.80 as of June 30, 2018.

e. **Wells Fargo account 5014** was opened on March 1, 2010, had a balance of $12,128.25 as of June 30, 2018.

f. **Wells Fargo account 5284** was opened on January 17, 2006, had a balance of $10,993.61 as of June 30, 2018.

g. From July 2017 through June 2018, $46,000 in cash deposits were made to **Wells Fargo account numbers 1890, 5284, 6631, 5014**. The business accounts did not have any transactions indicative of an actively operating business entity. For example, two of the purported business accounts (-**1890, -5014**) were inactive for well over a year before July 2017, when funds were transferred from those accounts to another account controlled by CAUDILLO, which he used to buy a house in Eureka, California. Since July, 2017,

sporadic cash deposits began to be made into both -**1890** and -**5014**. Similarly, another purported business savings account for "JC Greenhouse" (-**5284**) had sporadic cash and check deposits made to it, but none of the checks appeared to related a greenhouse business. Again, there were no withdrawals or disbursements from account -**5284** from February, 2014, until July, 2017, when a large outbound transfer was made and ultimately used to fund the purchase of the Eureka house. There were also no disbursements from -**5284** after the purchase of the home through June 2018, the date through which we have bank records.

TRAINING AND EXPERIENCE

51. Based on my training and experience, I know the following:

a. Individuals involved in fraud schemes like this one usually keep evidence of their schemes, such as pay-owe sheets for dividing the proceeds, contact information for their co-conspirators, and records documenting the scheme so when an error is made, they can recreate the documentation needed to help conceal the fraud.

b. These individuals often use the proceeds of the fraud to purchase expensive items, or store the proceeds in the form of cash to make it more difficult to trace.

c. Individuals involved in fraud schemes need to communicate with their co-conspirators about their fraudulent activity. There are usually records of those communications in their electronic devices such as cellular telephones.

d. Typically, they maintain the evidence where it is close at hand and safe, such as in their residences, vehicles, and digital devices, which are also commonly stored in their residences and vehicles. Such individuals commonly use digital devices to communicate with their fellow participants by phone, email and text messages. I know that individuals who commit crimes with the aid of electronic devices do not readily discard them, as computers, tablets and cell phones are expensive items that are typically used for years before being upgraded or discarded. Computers, tablets and cell phones can be used to communicate between co-conspirators and may contain information relating to the crime under investigation.

52. I know from training and experience that individuals involved in fraud keep the most damaging evidence and/or proceeds of the scheme at their residences, vehicles, garages and to help conceal the fraud from their fellow coworkers who may have access to such documents at the workplace. Proceeds such as cash and gifts are easier to conceal at the fraudster's residence rather than in plain view of coworkers. More sophisticated or cagey criminals may rent public storage units to use to further distance themselves from incriminating evidence, or safety deposit boxes, especially when storing valuables such as cash.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

53. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop,

notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and other involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital devices, operating system, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' X 35' X 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto

a hard drive, deleted, or viewed via the Internet.[1] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a

[1] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

controlled laboratory environment. Recovery can also require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and process on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created.

This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension of ".jpg" often times are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a

"dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

Request to Use Biometric Features to Unlock Digital Devices

54. Based on my training and experience, and knowledge of this investigation as discussed previously, I believe that digital devices, such as smartphones, will be found during the search.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric

features and enable the users of such devices to select which feature they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial

characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eye. Both the

Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello feature on older devices.

55. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

56. I also know from my training and experience, as well as from information found in publicly available materials include those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a

remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

57. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to the named targets of the investigation, (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

58. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

CONCLUSION

59. Based on the information set forth in this affidavit and my training and experience, I submit that there is probable cause to believe the SUBJECT PREMISES contains evidence, fruits, and instrumentalities of evidence of violations of 18 U.S.C. §§ 371, 1001, 1349, 1341, 1956, and 31 U.S.C. § 5324 (Conspiracy to Defraud the United States Government, False Statements, Conspiracy to Commit Mail Fraud, Money Laundering, and Structuring), and that SEIZABLE ACCOUNTS constitute and are derived from proceeds traceable to those violations, and are therefore subject to seizure pursuant to 21 U.S.C. § 853(f), 18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), 21 U.S.C. § 853, and 18 U.S.C. § 984.

_____
KELLY SHEN
U.S. POSTAL INSPECTOR

Subscribed and sworn to before me
this _____ day of November, 2018.

_____
UNITED STATES MAGISTRATE JUDGE